

Effective Hasse principle for the intersection of two quadrics

Tony Quertier
 Université de Caen Normandie, France
 tony.quertier@unicaen.fr

February 17, 2016

Abstract

We consider a smooth system of two homogeneous quadratic equations over \mathbb{Q} in $n \geq 13$ variables. In this case, the Hasse principle is known to hold, thanks to the work of Mordell in 1959. The only local obstruction is over \mathbb{R} . In this paper, we give an explicit algorithm to decide whether a nonzero rational solution exists, and if so, compute one.

1 Introduction

Let F_1, \dots, F_m be polynomials in the variables x_1, \dots, x_n with coefficients in a number field K . In the study of the resolution of the system $F_1(x_1, \dots, x_n) = \dots = F_m(x_1, \dots, x_n) = 0$, three very natural and well-studied problems are:

- LP (= Local problems): Decide whether solutions exist in every completion of K (\mathbb{R} , \mathbb{C} , p -adic fields, ...); if so, compute them.
- HP (= Hasse Principle): If LP is true, show the existence of a solution in K . Otherwise, there are clearly no solutions in K .
- EHP (= Effective HP): If solutions exist in K , compute one.

In this paper, we consider a smooth system of two homogeneous quadratic equations over $K = \mathbb{Q}$ in $n \geq 13$ variables. Before studying the case of two equations, it is worth recalling what is known in the case of a single quadratic equation.

Let $q(x_1, \dots, x_n)$ be a homogeneous quadratic form over \mathbb{Q} and $q(x_1, \dots, x_n) = 0$ the associated quadratic equation. The LP question was solved by the Chevalley-Waring theorem and by Hensel's lemma [7]. The corresponding algorithms are particularly efficient. The Hasse-Minkowski theorem asserts that HP holds for a single quadratic equation.

To solve EHP, Simon [8] and Castel [2] have written algorithms that quickly compute an explicit rational solution of $q(x_1, \dots, x_n) = 0$. Consequently, for a single quadratic equation, we consider the three problems solved and now focus on the case of two quadratic equations.

Let $q_0(x_1, \dots, x_n), q_1(x_1, \dots, x_n)$ be two quadratic forms over \mathbb{Q} . Demyanov [4] and Birch, Lewis and Murphy [1] solved LP for $n \geq 9$. Many people have

worked on the HP problem for two quadratic forms. Let us mention the most general results. Mordell settled the case $n \geq 13$ in 1959 [6]. His result was lowered down to $n \geq 11$ by Swinnerton-Dyer in 1964 [9], and later to $n \geq 9$ by Colliot-Thélène, Swinnerton-Dyer and Sansuc in 1987 [3]. In 2006, Wittenberg [10] proved that, if we assume Schinzel's hypothesis and the finiteness of Tate-Shafarevich groups of elliptic curves over number fields, then the HP holds as soon as $n \geq 6$.

To our knowledge, no work exists on the EHP problem for two quadratic equations. In this paper, we give explicit algorithms to solve EHP for $n \geq 13$. A non-negligible part of our work is based on [6].

In a preliminary part, we fix the notation and recall the notion of smoothness.

In part 3, we study the different signatures of the forms in the pencil, which govern the existence of a real solution. For this, we introduce the simultaneous block diagonalization of two quadratic forms and show the existence of a quadratic form with a convenient signature. This leads to a simple algorithm that decides the existence of a real solution.

In part 4, we give some low-level algorithms to split off a quadratic form into hyperbolic planes over \mathbb{R} or \mathbb{Q} . These rely on the ability to compute a solution for a single quadratic equation. Over \mathbb{Q} , as already mentioned, we may use the algorithm of Castel [2].

Part 5 is devoted to the computation of an explicit nontrivial real solution of the system.

In part 6, using this real solution, we can construct a rational totally isotropic subspace for $q_0(x)$ such that $q_1(x)$ is indefinite over this subspace.

In the last part 7, we use this subspace to derive a nontrivial rational solution of the system.

2 General notation

Let $K \supset \mathbb{Q}$ be a field. Let q_0 and q_1 be two quadratic forms over K in n variables. Using the canonical basis of K^n we have:

$$q_0(x) = \sum_{i,j=1}^n a_{ij}x_i x_j, \quad q_1(x) = \sum_{i,j=1}^n b_{ij}x_i x_j$$

with $a_{ij} = a_{ji}$ and $b_{ij} = b_{ji}$. We write $Q_0 = (a_{ij})$, $Q_1 = (b_{ij})$ the associated symmetric matrices. For $x = (x_1, \dots, x_n)$, we have

$$q_0(x) = xQ_0^t x, \quad q_1(x) = xQ_1^t x.$$

We also use the notation $q_0(x, y) = xQ_0^t y$ for the associated bilinear form.

Let

$$V = \{x \in \mathbb{P}^{n-1}(\overline{K}) \mid q_0(x) = q_1(x) = 0\}$$

be the projective variety defined by the two quadrics associated to q_0 and q_1 .

To study the intersection of two quadrics, it is necessary to study the pencil of quadrics through V . We denote by \mathcal{P}_K the pencil of quadrics associated to the pair (q_0, q_1) , that is the family of quadrics $a_0 q_0 + a_1 q_1 = 0$ with $(a_0 : a_1) \in \mathbb{P}^1(K)$. In practice, we will mainly consider this pencil for $K = \mathbb{Q}$ and $K = \mathbb{R}$. If

$\det(Q_0) = 0$, we replace q_0 by $a_0q_0 + a_1q_1$ for some $(a_0 : a_1) \neq (0 : 1)$ to assure that $\det(Q_0) \neq 0$ and similarly for Q_1 . From now on, we can set $\lambda = \frac{a_0}{a_1}$ and $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$: this is a polynomial of degree exactly n in λ .

We denote by $[r, s]$ the *signature* of a quadratic form q in n variables, where r is the positive component and s the negative component. If $\det(Q) \neq 0$, we have $r + s = n$, otherwise we have $r + s < n$.

We denote by \oplus the traditional *orthogonal sum* for quadratic forms. Moreover, for two matrices A and B , we define $A \oplus B$ the block diagonal matrix $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$.

The variety V is *smooth* if $q_0 = 0$ and $q_1 = 0$ intersect transversally *i.e.* if the rank of the Jacobian of q_0 and q_1 is equal to 2 at every point of V .

Hypothesis . We say that two quadratic forms q_0 and q_1 (resp. two symmetric matrices Q_0 and Q_1) defined over K , satisfy the *hypothesis H* if $\det(Q_0) \neq 0$, $\det(Q_1) \neq 0$, and V is smooth over K .

We know, for example from [5], that the variety V is smooth if and only if $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$ has only simple roots in \overline{K} . We have therefore the equivalent formulation:

Hypothesis . We say that two quadratic forms q_0 and q_1 (resp. two symmetric matrices Q_0 and Q_1) defined over K , satisfy the *hypothesis H* if $\det(Q_0) \neq 0$, $\det(Q_1) \neq 0$, and $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$ has only simple roots in \overline{K} .

3 Real quadratic forms

3.1 Simultaneous diagonalization

Proposition 1. Let Q_0 and Q_1 be two matrices of size n satisfying Hypothesis *H* over \mathbb{R} . Let m be the number of real roots of $\Delta(\lambda)$. There exists a matrix $P \in GL_n(\mathbb{R})$ such that PQ_0^tP is diagonal, with only ± 1 on the diagonal, and PQ_1^tP is a block diagonal matrix, with m first blocks of size 1 and then $(n-m)/2$ blocks of size 2 of the form

$$\begin{pmatrix} a & b \\ b & -a \end{pmatrix}.$$

Furthermore, each such block in PQ_1^tP is face to face with a block $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ in PQ_0^tP . Algorithm 1 computes such a matrix P .

Algorithm 1. Let Q_0 and Q_1 be two matrices of size n satisfying Hypothesis *H* over \mathbb{R} . This algorithm computes a matrix $P \in GL_n(\mathbb{R})$ satisfying the conclusion of Proposition 1.

1. Let $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$ and $\Lambda = \{\lambda_1, \dots, \lambda_n\}$ be the list of the roots of $\Delta(\lambda)$ such that $\lambda_1, \dots, \lambda_m \in \mathbb{R}$ and $\lambda_{m+i} = \overline{\lambda_{m+i+1}}$ for $i \geq 1$ odd.
2. For i from 1 to n , find a generator v_i of $\ker(\lambda_i Q_0 + Q_1)$ such that, for $i \leq m$, $v_i \in \mathbb{R}^n$.

3. Set $j = m + 1$. While $j < n$, set $w_j = \text{Re}(v_j)$, $w_{j+1} = \text{Im}(v_j)$ and $j = j + 2$.
4. For i from 1 to m , set $w_i = v_i$.
5. Let P be the square matrix of size n whose the i -th line is w_i , for $1 \leq i \leq n$. Set $Q'_0 = PQ_0^t P$.
6. For i odd from 1 to $n - m - 1$, apply the Jacobi's eigenvalues algorithm to diagonalize the block $(Q'_{0_{k,l}})_{m+i \leq k, l \leq m+i+1}$ and denote by P'_{m+i} the associated transformation matrix of size 2.
7. Set $P' = \text{Id}(m) \oplus \bigoplus_i P'_{m+i}$. Set $Q''_0 = P'Q'_0{}^t P'$ and $P = P'P$.
8. For i from 1 to n , divide the i -th line of P by $\sqrt{|Q''_{0_{ii}}|}$.
9. Return P .

Proof. In Step 2, the dimension of each kernel is 1 because $\Delta(\lambda)$ has only simple roots. We know that

$$v_i(\lambda_i Q_0) + v_i Q_1 = 0$$

then we have:

$$\begin{aligned} q_1(v_i, v_j) &= v_i Q_1^t v_j \\ &= v_i (-\lambda_i Q_0)^t v_j \\ &= -\lambda_i v_i Q_0^t v_j \\ &= -\lambda_i q_0(v_i, v_j) \end{aligned}$$

but we also have:

$$q_1(v_i, v_j) = -\lambda_j q_0(v_i, v_j).$$

We have $\lambda_i \neq \lambda_j$ for $i \neq j$, so we deduce that $q_0(v_i, v_j) = q_1(v_i, v_j) = 0$. Since the v_i are orthogonal for q_0 and q_1 , the w_i are also pairwise orthogonal for q_0 and q_1 , except maybe w_{m+i} and w_{m+i+1} , for i odd. The matrices Q'_0 and Q'_1 are therefore block diagonal with blocks of size 1 for each real root λ and of size 2 for each pair of conjugate complex roots. For i odd, from the equality $q_0(v_{m+i}, v_{m+i+1}) = 0$ we deduce that $q_0(w_{m+i}, w_{m+i+1}) = -q_0(w_{m+i+1}, w_{m+i+1})$. So, the shape of the blocks of size 2 associated to conjugate complex roots is:

$$\begin{pmatrix} a & b \\ b & -a \end{pmatrix}.$$

The same is true for Q'_1 . In Step 8, The Jacobi's eigenvalues algorithm computes an orthogonal matrix P'_{m+i} to diagonalize the blocks $A_i = (Q'_{0_{k,l}})_{m+i \leq k, l \leq m+i+1}$. We consider $B_i = (Q'_{1_{k,l}})_{m+i \leq k, l \leq m+i+1}$. Since, P'_{m+i} is orthogonal, we have:

$$\text{trace}(P'_{m+i} A_i^t P'_{m+i}) = \text{trace}(A_i P'_{m+i}{}^t P'_{m+i}) = \text{trace}(A_i) = 0$$

and then the shape of the blocks $P'_{m+i} A_i^t P'_{m+i}$ is always:

$$\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}.$$

Similarly, the shape of the $P'_{m+i} B_i^t P'_{m+i}$ is

$$\begin{pmatrix} c & d \\ d & -c \end{pmatrix}.$$

At the level of blocks, Step 8 divides the two lines of P'_{m+i} by the same constant $|a|$ therefore, the trace of the blocks is always zero. \square

3.2 Existence of a balanced quadratic form

Definition . We say that a quadratic form with signature $[r, s]$ is *balanced* if $|r - s| \leq 1$.

In this part we want to determine if a pair of quadratic forms has non trivial real solutions. After this we study the existence of a balanced quadratic form in the pencil $\mathcal{P}_{\mathbb{R}}$ and compute one if it exists.

Lemma 2 ((Cauchy's bound)). *Let $P(x) = x^n + a_{n-1}x^{n-1} \dots + a_0$ be a monic polynomial of degree n . If $x \in \mathbb{C}$ is a root of P then $|x| \leq 1 + \max_{1 \leq i \leq n} (|a_i|)$. The constant $a = 1 + \max_{1 \leq i \leq n} (|a_i|)$ is called Cauchy's bound of P .*

The next result follows easily from Proposition 1. We use the notation $r(\lambda_i^+)$ for $\lim_{\lambda \rightarrow \lambda_i, \lambda > \lambda_i} r(\lambda)$ and similarly for $r(\lambda_i^-)$ with $\lambda < \lambda_i$.

Theorem 3. *Let Q_0 and Q_1 be two matrices of size n satisfying Hypothesis H over \mathbb{R} . We denote by $\lambda_1 < \dots < \lambda_m$ the real roots of $\det(\lambda Q_0 + Q_1)$, $Q_{-\infty} = Q_0$ and $Q_{+\infty} = -Q_0$. We also denote by $[r(\lambda), s(\lambda)]$ the signature of $\lambda Q_0 + Q_1$ with $\lambda \in [-\infty, \infty]$. Then :*

1. *The signature of $\lambda Q_0 + Q_1$ is constant over the intervals $[-\infty, \lambda_1[$, $]\lambda_i, \lambda_{i+1}[$ and $]\lambda_m, \infty]$ for $i \in \{1, \dots, m-1\}$.*
2. *$r(\lambda_i^+) - r(\lambda_i^-) = -(s(\lambda_i^+) - s(\lambda_i^-))$.*
3. *$r(\lambda_i) = \frac{1}{2}(r(\lambda_i^+) + r(\lambda_i^-))$ and $s(\lambda_i) = \frac{1}{2}(s(\lambda_i^+) + s(\lambda_i^-))$.*

Corollary 4. *There exists $\lambda \in \mathbb{Q}$ such that $\lambda q_0 + q_1$ is balanced.*

Definition . We define the function $d : \mathbb{R} \rightarrow \mathbb{Z}$ by $d(\lambda) = r - s$, where $[r, s]$ is the signature of $\lambda q_0 + q_1$.

We can reformulate Theorem 3 using the function d .

Corollary 5. *The function d is piecewise constant with discontinuities at the roots of $\Delta(\lambda)$. The value of d at a discontinuity is the average of the two limit values of d on the left and on the right of this discontinuity.*

It is convenient for the next lemma to use the notation $\lambda_0 = -\infty$ and $\lambda_{n+1} = +\infty$.

Lemma 6. *Let Q_0 and Q_1 be two matrices of size n satisfying Hypothesis H over \mathbb{R} . Assume that $\Delta(\lambda)$ has $m \leq n$ real roots denoted by $\lambda_1 < \dots < \lambda_m$. We have:*

1. If $m \neq n$ then $\lambda Q_0 + Q_1$ is never definite.
2. If $m = n$, there exists at most one interval $]\lambda_i, \lambda_{i+1}[$ over which $\lambda Q_0 + Q_1$ is positive (resp. negative) definite. Moreover this interval is $]\lambda_s, \lambda_{s+1}[$ (resp. $]\lambda_r, \lambda_{r+1}[$) where $[r, s]$ is the signature of Q_0 .

Theorem 7. Let q_0 and q_1 be two quadratic forms of n variables. Then $V(\mathbb{R}) \neq \emptyset$ if and only if all the forms in $\mathcal{P}_{\mathbb{R}}$ are indefinite.

Two different proofs are done in [6] and [9].

Algorithm 2. Let Q_0 and Q_1 be two matrices of size n satisfying Hypothesis H over \mathbb{R} . This algorithm computes a rational number λ such that $\lambda Q_0 + Q_1$ is definite if there exists one, and returns a message otherwise.

1. Let a be Cauchy's bound of $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$ and I the interval $[-a - 1, a + 1]$.
2. Set m the number of real roots of Δ . If $m \neq n$, return a message saying that $\lambda Q_0 + Q_1$ is never definite.
3. Denote by $\lambda_1 < \dots < \lambda_n$ the roots of $\Delta(\lambda)$ and $[r, s]$ the signature of $-aQ_0 + Q_1$.
4. Let λ and μ be two rational numbers such that $\lambda \in]\lambda_r, \lambda_{r+1}[$ and $\mu \in]\lambda_s, \lambda_{s+1}[$.
5. If $\lambda Q_0 + Q_1$ is definite, return λ .
6. If $\mu Q_0 + Q_1$ is definite, return μ .
7. Return a message saying that $\lambda Q_0 + Q_1$ is never definite.

This algorithm is an effective test of Theorem 7. We are able to decide whether $V(\mathbb{R}) \neq \emptyset$ or equivalently q_0 and q_1 have a common nonzero real solution using this algorithm. The explicit construction of a real solution will be done in Algorithm 12 when $n \geq 3$.

Algorithm 3. Let Q_0 and Q_1 be two matrices of size n satisfying Hypothesis H over \mathbb{R} . This algorithm computes a rational number λ such that $\lambda Q_0 + Q_1$ is balanced and $\det(\lambda Q_0 + Q_1) \neq 0$.

1. Let a be Cauchy's bound of $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$.
2. Set $\lambda_{max} = a + 1$, $\lambda_{min} = -\lambda_{max}$, and $\lambda_b = 0$.
3. If $|d(\lambda_b)| \leq 1$ and $\Delta(\lambda_b) \neq 0$, return λ_b .
4. If $d(\lambda_b) = 0$, set $\lambda_{max} = \lambda_b$ and go to Step 7.
5. If $d(\lambda_b)$ and $d(\lambda_{min})$ have opposite signs, set $\lambda_{max} = \lambda_b$, else set $\lambda_{min} = \lambda_b$.
6. Set $\lambda_b = (\lambda_{min} + \lambda_{max})/2$ and go to Step 3.

Proof. Algorithm 3 simply makes a dichotomy over $[\lambda_{min}, \lambda_{max}]$ for function d , using the fact that $d(\lambda_{max}) = -d(\lambda_{min})$. \square

4 Reduction of a balanced quadratic form

Notation . We set K a field, with $K = \mathbb{R}$ or $K = \mathbb{Q}$. We denote by

$$\mathbb{H} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

the matrix associated to the quadratic form $2xy$: we call it a *hyperbolic plane*.

Now, we are going to give a set of algorithms to compute some transition matrix P such that PQ_0^tP is the block diagonal matrix $\mathbb{H} \oplus Q_2$. In this section, we only consider indefinite quadratic forms over K of dimension $n \geq 5$.

Notation . In this section, most algorithms take as an input a matrix $Q_0 = (a_{ij})$ associated to a quadratic form $\sum_{i,j=1}^n a_{ij}x_i x_j$ defined over K and compute a matrix $P \in GL_n(K)$. We denote by a'_{ij} the entries of PQ_0^tP .

Algorithm 4. Let $Q_0 = (a_{ij})$ be such that $\det(Q_0) \neq 0$ and y a nonzero vector in K^n such that $yQ_0^ty = 0$. This algorithm computes a matrix $P \in GL_n(K)$ such that $a'_{11} = 0$ and $a'_{12} \neq 0$.

1. Let P be a square matrix of size n having y as first line. Complete the matrix P to have $P \in GL_n(K)$.
2. Set $Q'_0 = PQ_0^tP$. Let $i \geq 2$ be the smallest index such that $(Q'_0)_{1i} \neq 0$, and P' be the transposition matrix which exchanges the second line with the i -th line.
3. Return $P = P'P$.

Algorithm 5. Let $Q_0 = (a_{ij})$ be such that $a_{11} = 0$ and $a_{12} \neq 0$. This algorithm computes a matrix $P \in GL_n(K)$ such that $a'_{11} = 0$, $a'_{12} = 1$, and $a'_{1i} = 0$ for $3 \leq i \leq n$.

1. Set $P = \text{Id}(n)$ and divide the first line of P by a_{12} .
2. Set $Q'_0 = PQ_0^tP$.
3. $P' = \text{Id}(n)$. For $i = 3$ to n , set $P'_{i2} = -(Q'_0)_{i1}$.
4. Return $P = P'P$.

Algorithm 6. Let $Q_0 = (a_{ij})$ be such that $a_{11} = 0$, $a_{12} = 1$, and $a_{1i} = 0$ for $3 \leq i \leq n$. This algorithm computes $P \in GL_n(K)$ such that PQ_0^tP is of the form $\mathbb{H} \oplus Q_2$.

1. Set $P = \text{Id}(n)$ and $S = \text{Id}(n)$.
2. For $i = 2$ to n , set $P_{i1} = -a_{i2}$. Set $Q_3 = PQ_0^tP$.
3. For $i = 1$ to n , set $S_{2i} = 2S_{2i} - (Q_3)_{22}S_{1i}$.
4. Set $S_{11} = 1/2$ and $P = SP$.
5. Return P .

Algorithm 7. Let $Q_0 = (a_{ij})$ and y be a nonzero vector in K^n such that $yQ_0^t y = 0$. This algorithm computes a matrix $P \in GL_n(K)$ such that $PQ_0^t P$ is of the form $\mathbb{H} \oplus Q_2$.

1. Apply Algorithm 4 to Q_0 and y , and denote by P the result.
2. Apply Algorithm 5 to $Q'_0 = PQ_0^t P$ and denote by P' the result.
3. Apply Algorithm 6 to $P'Q'_0{}^t P'$ and denote by P'' the result.
4. Return $P = P''P'P$.

Algorithm 8. Let $Q_0 = (a_{ij})$ of size $n \geq 5$ be defined over \mathbb{Q} and such that q_0 is balanced. This algorithm computes $P \in GL_n(\mathbb{Q})$ such that $PQ_0^t P$ is of the form $\mathbb{H} \oplus \dots \oplus \mathbb{H} \oplus Q_2$ where Q_2 is of size 3 if n is odd, or of size 4 if n is even.

1. Set $P = \text{Id}(n)$ and $i = 1$.
2. Extract the square submatrix $(Q_{0_{jk}})_{i \leq j, k \leq n}$ and denote it by Q_2 .
3. Compute a nonzero rational vector z such that $zQ_0^t z = 0$.
4. Apply Algorithm 7 to Q_2 and z , and denote by P' the result.
5. Set $C = \text{Id}(i-1) \oplus P'$.
6. Set $P = CP$, $Q_0 = CQ_0^t C$, $i = i + 2$.
7. If $n - i + 1 \geq 5$ go to Step 2.
8. Return P .

Remark . Step 3 can be done using the algorithm of Castel [2], that quickly computes a nonzero rational solution of a rational indefinite quadratic form of dimension $n \geq 5$.

The idea of this algorithm is based on [6]. The main idea is that after each loop the signature changes from $[r, s]$ to $[r-1, s-1]$. While the dimension of Q_2 is greater or equal to 5, we can continue because an indefinite quadratic form in $n \geq 5$ variables has always a nonzero rational solution.

5 Computation of a nonzero real solution of the system

To compute a nonzero real solution of the system of two quadratic forms, we study the nature of the roots of $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$. Obviously we consider that all the forms in $\mathcal{P}_{\mathbb{R}}$ are indefinite, otherwise $V(\mathbb{R})$ is clearly empty (see Theorem 7). In order to compute a real solution, we are going to first block diagonalize the two quadratic forms, and then find a solution using simple algorithms, depending on the number of real roots of $\Delta(\lambda)$.

Algorithm 9. Let q_0 and q_1 be two quadratic forms of the form

$$q_0(x, y, z, w) = x^2 - y^2 + z^2 - w^2,$$

$$q_1(x, y, z, w) = ax^2 - 2bxy - ay^2 + cz^2 - 2dzw - cw^2.$$

This algorithm computes a nonzero vector $v \in \mathbb{R}^4$ such that $q_0(v) = q_1(v) = 0$.

1. Set ε the sign of b and ε' the sign of d .
2. Compute a nonzero solution (x_1, w_1) of $|b|x^2 - |d|w^2 = 0$.
3. Return $v = (x_1, x_1, -\varepsilon\varepsilon'w_1, w_1)$.

Algorithm 10. Let q_0 and q_1 be two quadratic forms of the form

$$q_0(x, y, z) = x^2 + y^2 - z^2,$$

$$q_1(x, y, z) = \lambda_1 x^2 + ay^2 - 2byz - az^2.$$

This algorithm computes a nonzero vector $v \in \mathbb{R}^3$ such that $q_0(v) = q_1(v) = 0$.

1. If $a = \lambda_1$ return $(1, 0, 1)$.
2. Let denote by y_1, y_2 the real solutions of $(a - \lambda_1)y^2 - 2by - (a - \lambda_1) = 0$.
3. If $-y_1^2 + 1 \geq 0$ return $(\sqrt{-y_1^2 + 1}, y_1, 1)$.
4. Return $(\sqrt{-y_2^2 + 1}, y_2, 1)$.

Proof. If $a = \lambda_1$, $(1, 0, 1)$ is an obvious solution of the system. Otherwise, we see that the discriminant of

$$(a - \lambda_1)y^2 - 2by - (a - \lambda_1)$$

is $b^2 + (a - \lambda_1)^2 > 0$ hence y_1 and y_2 are real. We have $y_1 y_2 = -1$ and $y_1 + y_2 = \frac{2b}{a - \lambda_1}$, therefore $(-y_1^2 + 1)(-y_2^2 + 1) = -\frac{4b^2}{(a - \lambda_1)^2} - 1 < 0$. We deduce from this that $-y_1^2 + 1$ or $-y_2^2 + 1$ is nonnegative and it is easy to verify that the formula gives a solution. \square

Lemma 8. Let q_0 and q_1 be two quadratic forms of the form $q_0(x) = \sum_{i=1}^k x_i^2 - \sum_{j=k+1}^n x_j^2$, $q_1(x) = \sum_{i=1}^n b_i x_i^2$ satisfying Hypothesis H over \mathbb{R} . Let denote $m_- = \min(b_i \mid i \in \{k+1, \dots, n\})$ and $m_+ = \min(b_i \mid i \in \{1, \dots, k\})$. There exists a real λ such that $\lambda q_0 + q_1$ is a positive definite quadratic form if and only if $-m_- < m_+$.

Lemma 9. Let q_0 and q_1 be two quadratic forms of the form $q_0(x) = \sum_{i=1}^k x_i^2 - \sum_{j=k+1}^n x_j^2$, $q_1(x) = \sum_{i=1}^n b_i x_i^2$ satisfying Hypothesis H over \mathbb{R} . Let denote $m_- = \min(b_i \mid i \in \{k+1, \dots, n\})$ and $m_+ = \min(b_i \mid i \in \{1, \dots, k\})$. Let denote $M_- = \max(b_i \mid i \in \{k+1, \dots, n\})$ and $M_+ = \max(b_i \mid i \in \{1, \dots, k\})$. Then $V(\mathbb{R})$ is nonempty if and only if $-m_- \geq m_+$ and $-M_- \leq M_+$.

Algorithm 11. Let q_0 and q_1 be two quadratic forms of the form $q_0(x) = \sum_{i=1}^n a_i x_i^2$ with $a_i = \pm 1$, and $q_1(x) = \sum_{i=1}^n b_i x_i^2$ satisfying Hypothesis H over \mathbb{R} , and such that $V(\mathbb{R}) \neq \emptyset$. This algorithm computes a nonzero vector $w \in \mathbb{R}^n$ such that $q_0(w) = q_1(w) = 0$.

1. Let v_1 be the list of all the i such that $a_i = +1$ and v_2 the list containing the others.
2. Search M such that $b_M = \max_{i \in v_1}(b_i)$ and m such that $b_m = \min_{i \in v_1}(b_i)$.

3. If for all $k \in v_2$ we have $-b_k \notin [b_m, b_M]$ then set $q_0 = -q_0$ and go to Step 1.
4. Choose $k \in v_2$ such that $b_m \leq -b_k \leq b_M$.
5. If $b_m = -b_k$, set $x_m = 1$, $x_k = 1$ and $x_i = 0$ for the other i .
6. Otherwise, set $x_M = 1$, $x_m = \sqrt{\frac{-b_M - b_k}{b_m + b_k}}$, $x_k = \sqrt{x_m^2 + 1}$ and $x_i = 0$ for the other i .
7. Return (x_1, \dots, x_n) .

Proof. For Step 3, Lemma 9 assures that we can find k and k' in v_2 such that $-b_k \geq b_m$ and $-b_{k'} \leq b_M$. If $-b_k \leq b_M$ or $-b_{k'} \geq b_m$, we can go to Step 4. Otherwise we have $-b_{k'} \leq b_m \leq -b_k$. In this case, setting $q_0 = -q_0$ exchanges v_1 and v_2 , so that the actual value of m will provide us with a solution for k for the new Step 3. For Step 5, $(b_M + b_k)$ and $(b_m + b_k)$ have opposite signs and it is an easy exercise to verify that Steps 5 and 6 give us a solution. \square

Algorithm 12. Let Q_0 and Q_1 be two matrices of size n satisfying Hypothesis H over \mathbb{R} and such that $V(\mathbb{R}) \neq \emptyset$. This algorithm computes a nonzero $y \in \mathbb{R}^n$ such that $q_0(y) = q_1(y) = 0$.

1. Set $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$.
2. Set a the number of real roots of $\Delta(\lambda)$.
3. Apply Algorithm 1 to Q_0 and Q_1 . Denote by P the result.
4. Set $Q'_0 = PQ_0^t P$ and $Q'_1 = PQ_1^t P$.
5. If $a = 0$, apply Algorithm 9 to $(Q'_{0_{ij}})_{1 \leq i, j \leq 4}$ and $(Q'_{1_{ij}})_{1 \leq i, j \leq 4}$. Denote by y the result and set $z = (y_1, y_2, y_3, y_4, 0, \dots, 0)$.
6. If $a = 13$ apply Algorithm 11 to Q'_0 and Q'_1 . Denote by z the result.
7. In $0 < a < 13$, apply Algorithm 10 to $(Q'_{0_{ij}})_{a \leq i, j \leq a+2}$ and $(Q'_{1_{ij}})_{a \leq i, j \leq a+2}$. Denote by (z_a, z_{a+1}, z_{a+2}) the result. Set $z = (0, \dots, 0, z_a, z_{a+1}, z_{a+2}, 0, \dots, 0)$.
8. Return $z \cdot P$.

6 A suitable change of basis

In this section, we give some algorithms to construct a rational totally isotropic subspace of $q_0(x)$ such that $q_1(x)$ is indefinite over this subspace. We keep the notation of the previous section concerning the inputs and outputs of the algorithms.

Algorithm 13. Let $Q_0 = (a_{ij})$ be such that $a_{11} = 0$ and $a_{13} \neq 0$. This algorithm computes a matrix $P \in GL_n(K)$ such that $a'_{11} = 0$, $a'_{12} = 0$, $a'_{13} = 1$, and $a'_{1i} = 0$ for $4 \leq i \leq n$. Moreover, the first two columns of P are the same as in $\text{Id}(n)$.

1. Set $P = \text{Id}(n)$ and divide the third line of P by a_{13} .

2. Set $Q'_0 = PQ_0^t P$.
3. Set $P' = \text{Id}(n)$. Set $P'_{23} = -(Q'_0)_{12}$, and for $i = 4$ to n , $P'_{i3} = -(Q'_0)_{i1}$.
4. Return $P = P'P$.

Algorithm 14. Let Q_0 and Q_1 be two matrices of size $n \geq 3$ satisfying Hypothesis H over \mathbb{R} and such that $V(\mathbb{R}) \neq \emptyset$. Let a nonzero $z \in \mathbb{R}^n$ be such that $q_0(z) = 0$ and $q_1(z) = 0$. This algorithm computes a matrix $P \in GL_n(\mathbb{R})$ such that the first line of $PQ_0^t P$ (resp. $PQ_1^t P$) is $(0, 1, 0, \dots, 0)$ (resp. $(0, 0, 1, 0, \dots, 0)$).

1. Apply Algorithm 4 to Q_0 and z , and denote by P the result.
2. Set $Q'_0 = PQ_0^t P$ and $Q'_1 = PQ_1^t P$.
3. Apply Algorithm 5 to Q'_0 and denote by P' the result.
4. Set $P = P'P$ and $Q''_1 = P'Q'_1{}^t P'$.
5. Let $i \geq 3$ be the smallest index such that $(Q''_1)_{1i} \neq 0$, and P'' be the transposition matrix which exchanges the third line with the i -th line. Set $P = P''P$.
6. Apply algorithm 13 to $P''Q''_1{}^t P''$ and denote by R the result. Set $P = RP$.
7. Return P .

Proof. This algorithm is straightforward, until Step 4. At this step the first line of $PQ_0^t P$ is $(0, 1, 0, \dots, 0)$ and the first line of Q'_1 is $(0, *, \dots, *)$. For Step 5, certainly there exists an index $i \geq 2$ such that $(Q''_1)_{1i} \neq 0$ because $\det(Q_1) \neq 0$. The index $i = 2$ cannot be the only one because otherwise z would be a singular point of V , contradicting the smoothness of V . This proves that Step 5 is always possible. For Step 6, the matrix R does not change the first line of Q''_0 because the first two columns of R are the same as in $\text{Id}(n)$. \square

Algorithm 15. Let $Q_0 = (a_{ij})$ and $Q_1 = (b_{ij})$ be two matrices of size $n \geq 5$ satisfying Hypothesis H over \mathbb{R} . Let a nonzero $z \in \mathbb{R}^n$ be such that $q_0(z) = 0$ and $q_1(z) = 0$. This algorithm computes a nonzero $z^- \in \mathbb{R}^n$ such that $q_0(z^-) = 0$ and $q_1(z^-) < 0$.

1. Apply Algorithm 14 to Q_0 , Q_1 and z . Denote by P the result and set $Q'_0 = PQ_0^t P$ and $Q'_1 = PQ_1^t P$.
2. Extract the submatrix $(Q'_{0_{ij}})_{2 \leq i, j \leq n}$ of Q'_0 , denote it by F and let $f(x)$ be the associated quadratic form.
3. Extract the submatrix $(Q'_{1_{ij}})_{2 \leq i, j \leq n}$ of Q'_1 , denote it by G and let $g(x)$ be the associated quadratic form.
4. If $F_{22} = 0$, set $z = ((-1 - G_{22})/2, 0, 1, 0, \dots, 0)$ and go to Step 8.
5. Denote by ε the sign of F_{22} . Set $y_1 = 1$, $y_2 = \varepsilon$, and for $i = 3$ to $n - 1$, set $y_i = 0$.

6. While $g(y) - y_2 f(y) \geq 0$, set $y_2 = 2y_2$.

7. Set $z = (-f(y)/2, y_1, \dots, y_{n-1})$.

8. Return $z^- = z \cdot P$.

Proof. At the end of Step 3 we have:

$$\begin{aligned} q'_0(x) &= 2x_1x_2 + f(x_2, \dots, x_n) \\ q'_1(x) &= 2x_1x_3 + g(x_2, \dots, x_n) \end{aligned}$$

For Step 4, we have $q'_0(z) = 0$ and $q'_1(z) = -1$. Otherwise, we consider the function:

$$h(x) = x_2g(x) - x_3f(x).$$

This is a polynomial of degree 3 in x_3 and the leading coefficient is $-F_{22}$. So, $h(x)$ is negative for $x_3 = \varepsilon x'_3$ with $x'_3 > 0$ large enough. Setting at last $y = (1, \varepsilon x'_3, 0, \dots, 0)$ and $z = (-f(y)/2, 1, \varepsilon x'_3, 0, \dots, 0)$, we have $q'_0(z) = 0$ and $q'_1(z) = -\varepsilon x'_3 f(y) + g(y) < 0$. □

Algorithm 16. Let $Q_0 = (a_{ij})$ and $Q_1 = (b_{ij})$ be two matrices of size $n \geq 5$, a nonzero $y \in \mathbb{R}^n$ be such that $q_0(y) = 0$ and $q_1(y) < 0$. This algorithm computes a $z \in \mathbb{Q}^n$ such that $q_0(z) = 0$, $q_1(z) < 0$.

1. Compute a rational nonzero solution w of $q_0(w) = 0$ and apply Algorithm 7 over \mathbb{Q} to Q_0 and w . Denote by P' the result. Set $Q'_0 = P'Q_0^t P'$, $Q'_1 = P'Q_1^t P'$, and $y' = y \cdot P'^{-1}$.
2. If $y'_i = 0$ for all $i \geq 2$, return $(1, 0, \dots, 0)P'$.
3. Denote $i \geq 2$ the smallest index such that $y'_i \neq 0$. We set P'' the permutation matrix that exchanges the second line with the i -th. Set $P = P''P'$, $y'' = y' \cdot P''$, $Q''_0 = P''Q'_0{}^t P''$, $Q''_1 = P''Q'_1{}^t P''$, and $\varepsilon = \frac{|y''_2|}{2}$.
4. Extract the submatrix $(Q''_{0_{ij}})_{3 \leq i, j \leq n}$ of Q''_0 , denote it by F and let $f(x)$ be the associated quadratic form.
5. For $i = 1$ to n , choose a rational number z''_i such that $|y''_i - z''_i| < \varepsilon$. If $q''_1(z'') \geq 0$, set $\varepsilon = \varepsilon/2$ and go to Step 5.
6. Set $u_1 = \frac{-f(z''_3, \dots, z''_n)}{2z''_2}$ and $u = (u_1, z''_2, \dots, z''_n)$.
7. If $q''_1(u) < 0$, return $u \cdot P$. Otherwise, set $\varepsilon = \varepsilon/2$ and go to Step 5.

Proof. After Step 4, we have $q''_0(y'') = q_0(y) = 0$ and $q''_1(y'') = q_1(y) < 0$ with $Q''_0 = \mathbb{H} \oplus F$. Step 5 is possible because the function q''_1 is continuous and the set \mathbb{Q} is dense in \mathbb{R} . Because $\varepsilon \leq |y''_2|$, we have $z''_2 \neq 0$. Since $Q''_0 = \mathbb{H} \oplus F$, the formula in Step 6 gives $q''_0(u) = 0$. As y'' also satisfies the relation $y''_1 = \frac{-f(y''_3, \dots, y''_n)}{2y''_2}$, by continuity we deduce that, when ε is small enough, u_1 is close to y''_1 so that u is close to y'' and $q''_1(u) < 0$. □

7 Computation of a nonzero rational solution

Algorithm 17. Let Q_0 and Q_1 be two matrices of size $n \geq 13$ satisfying Hypothesis H over \mathbb{Q} and such that $V(\mathbb{R}) \neq \emptyset$. This algorithm computes a nonzero $x \in \mathbb{Q}^n$ such that $q_0(x) = q_1(x) = 0$.

1. Apply Algorithm 3 and find $\lambda_0 \in \mathbb{Q}$ such that $Q_0 + \lambda_0 Q_1$ is balanced and has nonzero determinant. Set $Q_0 = Q_0 + \lambda_0 Q_1$.
2. Compute a nonzero solution $y \in \mathbb{Q}^n$ of $q_0(y) = 0$.
3. If $q_1(y) = 0$ return y . If $q_1(y) < 0$ set $Q_1 = -Q_1$.
4. Apply Algorithm 12 to Q_0 and Q_1 . Denote by u the result.
5. Apply Algorithm 15 to (Q_0, Q_1, u) and denote by v the result.
6. Apply Algorithm 16 to (Q_0, Q_1, v) and denote by z the result.
7. While $q_0(y, z) = 0$, do
 - (a) Choose $y' \in \mathbb{Q}^n$ randomly until $q_0(y, y') \neq 0$.
 - (b) Set $w = y' - \frac{q_0(y, y')}{2q_0(y, y')} y$.
 - (c) If $q_1(w) = 0$ return w .
 - (d) If $q_1(w) > 0$ set $y = w$ otherwise set $z = w$.
8. Let $P^{(1)}$ be a matrix whose the first $n-2$ lines generate the solutions in x of $xQ_0^t y = xQ_0^t z = 0$, and whose the last two lines are y and z .
9. Set $Q_0^{(1)} = P^{(1)} Q_0^t P^{(1)}$, $Q_1^{(1)} = P^{(1)} Q_1^t P^{(1)}$.
10. Set $P^{(2)}$ the permutation matrix that exchanges the first line with the $(n-1)$ -th line and the second line with the n -th line.
11. Set $Q_0^{(2)} = P^{(2)} Q_0^{(1)t} P^{(2)}$, $Q_1^{(2)} = P^{(2)} Q_1^{(1)t} P^{(2)}$ and $P = P^{(2)} P^{(1)}$.
12. Extract the submatrix $(Q_{0_{ij}}^{(2)})_{3 \leq i, j \leq n}$ of $Q_0^{(2)}$, denote it by Q_2 .
13. Apply Algorithm 8 to Q_2 and denote by P' the result.
14. Set $P^{(3)} = \text{Id}(2) \oplus P'$, $Q_0^{(3)} = P^{(3)} Q_0^{(2)t} P^{(3)}$, $Q_1^{(3)} = P^{(3)} Q_1^{(2)t} P^{(3)}$ and $P = P^{(3)} P$.
15. If $(Q_1^{(3)})_{33} > 0$, compute a nonzero rational solution of $q_1^{(4)}(x) = 0$ of the form $x = (0, x_2, x_3, 0, x_5, 0, x_7, 0, x_9, 0, 0, 0, \dots)$. Otherwise, compute a nonzero rational solution of $q_1^{(4)}(x) = 0$ of the form $x = (x_1, 0, x_3, 0, x_5, 0, x_7, 0, x_9, 0, 0, 0, \dots)$.
16. Return xP .

Theorem 10. Let $q_0(x)$ and $q_1(x)$ be two indefinite rational quadratic form in $n \geq 13$ variables satisfying Hypothesis H over \mathbb{Q} and such that $V(\mathbb{R})$ is not empty. Then there exists a nonzero rational solution x of $q_0(x) = q_1(x) = 0$. Moreover Algorithm 17 computes such a solution.

Proof. After Step 1, $q_0(x)$ is balanced, so that in Step 2, such a rational y exists and after Step 3, we have $q_1(y) > 0$. For Step 4 such a real solution exists because $V(\mathbb{R})$ is nonempty. Steps 4,5 and 6 compute a rational vector z such that $q_0(z) = 0$ and $q_1(z) < 0$. Step 7 assures us that y and z are not orthogonal for q_0 , then the intersection of $\langle y, z \rangle$ and $\langle y, z \rangle^{\perp_{q_0}}$ is nonzero. Therefore the matrix $P^{(1)}$ of Step 8 is invertible. Step 13 is possible because $Q_0^{(2)} = \mathbb{H} \oplus Q_2$ is balanced with signature $[r, s]$ thus Q_2 is balanced with signature $[r - 1, s - 1]$ and dimension $n - 2 \geq 11$. The subspaces of the elements of the form $x = (0, x_2, x_3, 0, x_5, 0, x_7, 0, x_9, 0, 0, 0, \dots)$ and $x = (x_1, 0, x_3, 0, x_5, 0, x_7, 0, x_9, 0, 0, 0, \dots)$ are both totally isotropic for $q_0^{(4)}$. To conclude we just need to compute a solution of $q_1^{(4)}(x) = 0$ in one of these subspaces. Since $(Q_1^{(4)})_{11} > 0$ and $(Q_1^{(4)})_{22} < 0$, the choice made in Step 15 assures that $q_1^{(4)}(x)$ is indefinite on this subspace. Moreover, in this subspace $q_1^{(4)}(x)$ has 5 variables and, by the Hasse principle, has rational solutions. This concludes the proof. \square

References

- [1] B. J. Birch and D. J. Lewis, and T. G. Murphy, ‘Simultaneous quadratic forms’, *Amer. J. Math.* (1962).
- [2] P. Castel, ‘Solving quadratic equations in dimension 5 or more without factoring’, *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium* (2013).
- [3] J.-L. Colliot-Thélène, and J.-J. Sansuc, and H. P. F. Swinnerton-Dyer, ‘Intersections de deux quadriques et surfaces de Châtelet’, *C. R. Acad. Sci. Paris Sér. I Math.* (1984).
- [4] V. B. Demyanov, ‘Pairs of quadratic forms over a complete field with discrete norm with a finite field of residue classes’, *Izv. Akad. Nauk SSSR. Ser. Mat.* (1956).
- [5] J. Harris, ‘Algebraic geometry’, *Springer-Verlag, New York* (1995).
- [6] L. J. Mordell, ‘Integer solutions of simultaneous quadratic equations’, *Abh. Math. Sem. Univ. Hamburg* (1959).
- [7] J.-P. Serre, ‘A Course in Arithmetic’, *Springer* (1996).
- [8] D. Simon, ‘Solving quadratic equations using reduced unimodular quadratic forms’, *Mathematics of Computation* (2005).
- [9] H. P. F. Swinnerton-Dyer, ‘Rational zeros of two quadratic forms’, *Acta Arith* (1964).
- [10] O. Wittenberg, ‘Principe de Hasse pour les intersections de deux quadriques’, *C. R. Math. Acad. Sci. Paris* (2006).